# Noteworthy
## Application Service Provider Privacy & Security Policies

| | |
|---|---|
| **Access** | As a CCHIT 2006 and 2007 certified product, NetPracticeEHR has demonstrated compliance with the increasingly stringent security and documentation requirements set forth. CCHIT's test criteria are based, in part, upon HIPAA 164.310 (Physical Safeguards) and HIPAA 164.312 (Technical Safeguards). Noteworthy's intention is to stay current with CCHIT certification, meaning that it will continue to support and enhance system features related to HIPAA compliance.<br><br>Patient data in Noteworthy Medical Systems products is fully protected against unauthorized access. This involves the combination of physical security of servers and backup media, a 3-tier firewall/access system for access to the servers, security policies, 128 bit encryption and mechanisms with include locking out a user after 3 unsuccessful login attempts.<br><br>Full-time personnel monitor security to prevent unauthorized access to the network and any patient data. Security patches are installed weekly and/or daily as they become available. A firewall filters malicious content and ensures proper encryption is being used.<br><br>Servers and network equipment are physically secured and those servers that house applications and patient data are isolated from other servers and equipment. |
| **Authorization** | Noteworthy Medical Systems products provide feature-by-feature control systems to regulate user access to individual features, and clients can determine which users have access. Access levels may be configured to support the minimum necessary requirements for different user types throughout your enterprise. All passwords are encrypted, and the system provides automatic system lock and automatic system logoff, which can be set for varying levels of inactivity. |
| **Authentication** | NetPracticeEHR is CCHIT 2007 certified and meets all of the stringent security requirements set forth in the requirements. Users must authenticate with an industry-standard username/password combination, and practices have full control over password expiration rules, login retry limits (before lockout), and screen locking rules. All of our networks and servers use standard encryption protocols to prevent password sniffing and/or network-level attacks. |

| | |
|---|---|
| **Audit** | Noteworthy Medical Systems products keep an audit trail of each access to patient data and all disclosures of patient data, in accordance with HIPAA guidelines and CCHIT 2007 requirements.<br><br>NetPracticeEHR provides a complete audit trail detailing each time a patient's record was accessed or updated, including the patient, user, data accessed, date and time. Audit events are automatically collected by each of the program components and reported to an audit service. Audit events are managed and viewed through NetPracticeEHR's web administration console providing extensive audit trails. These services exceed CCHIT 2007 requirements. |
| **Secondary Uses of Data** | Noteworthy Medical Systems does not sell customer data under any circumstances nor is it used for marketing of any kind. NetPracticeEHR does not allow outside access to our customers' data in any way.<br><br>The customer has control of who has access to their data via a combination of the "User Admin" function and the "Permissions-Sharing" function.<br><br>Noteworthy Medical Systems does not use data for Public Health Reporting |
| **Data Ownership** | Indentified patient and user data that are entered into the NetPracticeEHR system are the exclusive property of and are owned by the customer.<br><br>Derived data, such as metrics, statistics and user supplied data that is put into the system on a global level, and which is de-identified, are owned by Noteworthy Medical Systems.<br><br>In the event a current customer leaves a practice or decides to use a different EHR, Noteworthy will provide that customer with their data in a suitable electronic format under the terms and conditions of the original sales agreement. |